Electronic Version

Stylesheet Version v1.1.1

Claims

[c1] A smartcard transaction system configured with a biometric security system, said system comprising:
a smartcard configured to communicate with a reader;
a reader configured to communicate with said system;
a voice print sensor configured to detect a proffered voice print sample, said voice print sensor configured to communicate with said system; and,
a device configured to verify said proffered voice print sample to facilitate a transaction.

[c2] The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

[c3] The smartcard transaction system of claim 1, wherein said voice print sensor is configured to facilitate a finite number of scans.

[c4] The smartcard transaction system of claim 1, wherein said voice print sensor is configured to log at least one of a detected voice print sample, processed voice print sample and stored voice print sample.

[c5] The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered voice print samples, proffered and registered user information, terrorist information, and criminal information.

[c6] The smartcard transaction system of claim 5, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c7] The smartcard transaction system of claim 6, wherein said remote database is configured to be operated by an authorized sample receiver.

[c8] The smartcard transaction system of claim 1, wherein said voice print sensor device is configured with an audio capture device.

[c9] The smartcard transaction system of 8, wherein said audio capture device is at least one of a microphone, telephone, cellular phone, computer and voice recorder.

[c10] The smartcard transaction system of claim 1, wherein said voice print sensor is configured to detect and verify voice print characteristics including at least one of voice

print waveforms in the time domain, energy content in the voice prints across the frequency domain, stochastic models of the voice print, and template models of the voice print.

[c11] The smartcard transaction system of claim 1, wherein said voice print sensor device is configured to detect and verify audio noise associated with an electronic device, motion, and body heat.

[c12] The smartcard transaction system of claim 1, further including a device configured to compare a proffered voice print sample with a stored voice print sample.

[c13] The smartcard transaction system of claim 12, wherein said device configured to compare a voice print sample is at least one of a third-party security vendor device and local CPU.

[c14] The smartcard transaction system of claim 12, wherein a stored voice print sample comprises a registered voice print sample.

[c15] The smartcard transaction system of claim 14, wherein said registered voice print sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account informa-

tion, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c16] The smartcard transaction system of claim 15, wherein different registered voice print samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c17] The smartcard transaction system of claim 15, wherein a voice print sample is primarily associated with first user information wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a voice print sample is secondarily associated with second user information wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account infor-

mation, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

[c18] The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered voice print sample.

[c19] The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered voice print sample.

[c20] The smartcard transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

[c21] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c22] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

[c23] A method for facilitating biometric security in a smart-card transaction system comprising: proffering a voice print to a voice print sensor communicating with said system to initiate verification of a voice print sample for facilitating authorization of a transaction.

[c24] The method for of claim 23, further comprising registering at least one voice print sample with an authorized sample receiver.

[c25] The method of claim 24, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a voice print to said authorized sample receiver, processing said voice print to obtain a voice print sample, associating said voice print sample with user information, verifying said voice print sample, and storing said voice print sample upon verification.

[c26] The method of claim 23, wherein said step of proffering includes proffering a voice print to at least one of a microphone, telephone, cellular phone, computer and voice recorder.

[c27] The method of claim 23, wherein said step of proffering further includes proffering a voice print to a voice print sensor communicating with said system to initiate at

least one of: storing, comparing, and verifying said voice print sample.

[c28] The method of claim 23, wherein said step of proffering a voice print to a voice print sensor communicating with said system to initiate verification further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c29] The method of claim 23, wherein said step of proffering a voice print to a voice print sensor communicating with said system to initiate verification further includes comparing a proffered voice print sample with a stored voice print sample.

[c30] The method of claim 29, wherein said step of comparing includes comparing a proffered voice print sample to a stored voice print sample by using at least one of a third-party security vendor device and local CPU.

[c31] The method of claim 29, wherein said step of comparing includes comparing voice print characteristics including at least one of voice print waveforms in the time domain, energy content in the voice prints across the frequency domain, stochastic models of the voice print, and tem-

plate models of the voice print.

[c32] The method of claim 23, wherein said step of proffering a voice print to a voice print sensor communicating with said system further comprises using said voice print sensor to detect at least one of audio noise associated with an electronic device, motion, and body heat.

[c33] The method of claim 23, wherein said step of proffering a voice print to a voice print sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered voice print sample.

[c34] The method of claim 23, wherein said step of proffering a voice print to a voice print sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure.

[c35] A method for facilitating biometric security in a smartcard transaction system comprising:
detecting a proffered voice print at a sensor communicating with said system to obtain a proffered voice print sample;
verifying the proffered voice print sample; and
authorizing a transaction to proceed upon verification of the proffered voice print sample.

[c36] The method of claim 35, wherein said step of detecting further includes detecting a proffered voice print at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

[c37] The method of claim 35, wherein said step of detecting a proffered voice print includes detecting a proffered voice print at one of a microphone, telephone, cellular phone, computer and voice recorder.

[c38] The method of claim 35, wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered voice print sample.

[c39] The method of claim 35, wherein said step of detecting further includes receiving a finite number of proffered voice print samples during a transaction.

[c40] The method of claim 35, wherein said step of detecting further includes logging each proffered voice print sample.

[c41] The method of claim 35, wherein said step of detecting further includes at least one of detection, processing and storing at least one second proffered voice print sample.

[c42] The method of claim 35, wherein said step of detecting further includes using said voice print sensor to detect at

least one of audio noise associated with an electronic device, motion, and body heat.

[c43] The method of claim 35, wherein said step of verifying includes comparing a proffered voice print sample with a stored voice print sample.

[c44] The method of claim 43, wherein said step of comparing a proffered voice print sample with a stored voice print sample comprises storing, processing and comparing at least one voice print characteristic including voice print waveforms in the time domain, energy content in the voice prints across the frequency domain, stochastic models of the voice print, and template models of the voice print.

[c45] The method of claim 43, wherein comparing a proffered voice print sample with a stored voice print sample includes comparing a proffered voice print sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

[c46] The method of claim 35, wherein said step of verifying includes verifying a proffered voice print sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

[c47] The method of claim 35, wherein said step of verifying includes verifying a proffered voice print sample using one of a local CPU and a third-party security vendor.